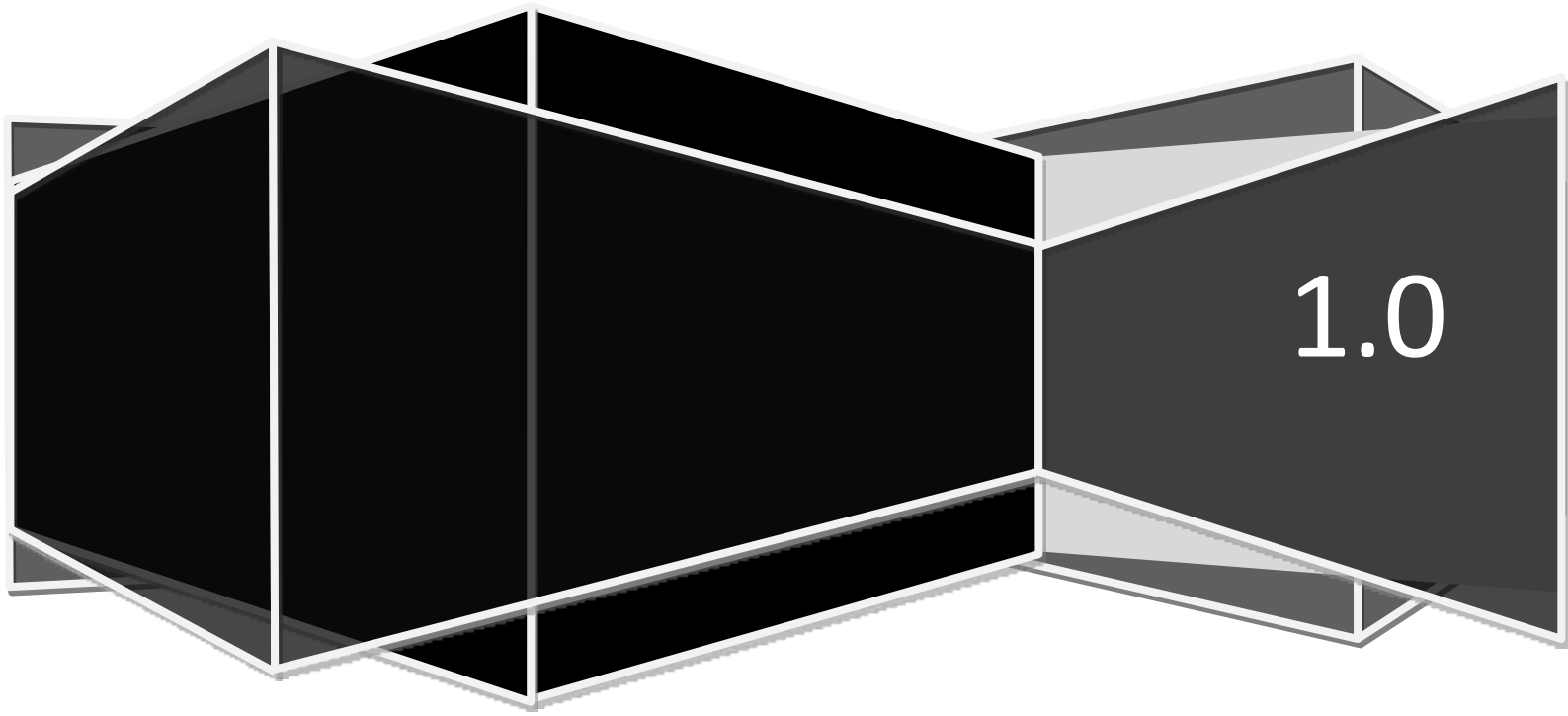
Segurança da Informação

Pilares e conceitos de proteção e segurança

Prof. Wagner Bugs



Conteúdo

Segurança da Informação.....2
Criptografia.....3
Firewalls (Parede de Fogo).....5
Atacantes ou Invasores.....6
Códigos Maliciosos.....7
Questões de Proteção e Segurança.....9

SEGURANÇA DA INFORMAÇÃO

Introdução

A Segurança da Informação é um conjunto de princípios, técnicas, protocolos, normas e regras que visam garantir um melhor nível de confiabilidade. Tudo isso se tornou necessário com a grande troca de informações entre os computadores com as mais variadas informações (transações financeiras e até uma simples conversação em salas de bate-papo) e principalmente pela vulnerabilidade oferecida pelos sistemas.

Princípios da Segurança da Informação

- *Confidencialidade*: É a garantia de que os dados serão acessados apenas por usuários autorizados. Geralmente, restringindo o acesso mediante o uso de um nome de usuário e senha.
- *Integridade*: É a garantia de que a mensagem não foi alterada durante a transmissão, ou seja, é a garantia da exatidão e completeza da informação.
- *Disponibilidade*: É a garantia de que um sistema estará sempre disponível a qualquer momento para solicitações.
- *Autenticidade*: É a garantia de que os dados fornecidos são verdadeiros ou que o usuário é o usuário legítimo.
- *Não Repúdio*: é a garantia de que uma pessoa não consiga negar um ato ou documento de sua autoria. Essa garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não-repúdio quando houver Autenticidade e Integridade (ou seja, quando for possível determinar quem mandou a mensagem e quando for possível garantir que a mensagem não foi alterada).

Vulnerabilidade

Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Existem casos onde um software ou sistema operacional instalado em um computador pode conter uma vulnerabilidade que permite sua exploração remota, ou seja, através da rede. Portanto, um atacante conectado à Internet, ao explorar tal vulnerabilidade, pode obter acesso não autorizado ao computador vulnerável.

Senhas

A senha (password) é um dos métodos mais utilizados na Internet ou sistemas computacionais para autenticar um usuário. Essa senha é exigida para garantir que o usuário é o usuário legítimo. Porém, a senha pode ser obtida por terceiros utilizando técnicas *hacking.* Estas técnicas podem ser a utilização de ferramentas de força bruta (esta técnica visa realizar tentativas de acesso baseado em regras) ou utilizando a fragilidade de um serviço ou sistema oferecido. Por esta razão, a elaboração de uma boa senha pode minimizar ou em alguns casos anular qualquer tentativa de obtenção desta senha.

As técnicas de força bruta utilizam regras específicas para a obtenção das senhas. Elaborar uma boa e longa (mínimo de 8 caracteres) senha, mesclando letras (maiúsculas e minúsculas), números e caracteres especiais, pode retardar estas técnicas fora de um tempo hábil, podendo levar meses ou anos.

Evite criar senhas com palavras simples ou apenas números. Mesclar letras e números oferece uma leve proteção. Alternar entre letras maiúsculas, minúsculas e números seria mais eficiente. Porém, para criar senhas com um nível maior de segurança devemos mesclar letras (maiúsculas e minúsculas), números e caracteres especiais. O tamanho da senha também é importante. Devemos criar senhas com no mínimo 8 caracteres.

Exemplo de senhas inseguras e seguras:

- Inseguras: meumor16, forever, 1a2m3o4r, 123eja, aq1sw2, etc.
- Seguras: ?F2eR7##u5a, #Pu63j?#fP!, etc.

Outras falhas comuns dos usuários é utilizar os recursos oferecidos para a recuperação de como Pergunta Secreta entre outros recursos. Muitos usuários cadastram perguntas como “Cidade onde minha mãe nasceu?” ou “Nome da minha primeira professora?” ou ainda “Meu time de futebol favorito?”. Em alguns casos, o atacante nem precisar ir tão longe para obter estas informações. Visitando sites de relacionamento como o Orkut onde estas informações estão explicitamente exibidas. O atacante poderia também obter estas informações através de engenharia social.

A dica seria cadastrar uma resposta não condizente com a pergunta secreta. Por exemplo, “Qual a cidade que minha mãe nasceu?” Resposta: Eu gosto de Lasanha.

CRIPTOGRAFIA

Criptografia é a ciência ou arte de escrever mensagens em forma cifrada ou em código. Basicamente, é o método utilizado para alterar os caracteres originais de uma mensagem por outros caracteres, ocultando a mensagem. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- Autenticar a identidade de usuários;
- Autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- Proteger a integridade de transferências eletrônicas de fundos.

Uma mensagem codificada por um método de criptografia deve ser sigilosa, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser assinada, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e/ou ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais chaves. A chave é uma seqüência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizada pelos métodos de criptografia para criptografar e descriptografar mensagens.

Criptografia de chave única (simétrica)

A criptografia de chave única utiliza a mesma chave tanto para criptografar quanto para descriptografar mensagens. Apesar de este método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas. Utilizada normalmente em redes de computadores por ser mais simples a administração.

Criptografia de chaves pública e privada (assimétrica)

A criptografia de chaves pública e privada utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens.

Chave pública: Pública no que se refere ao grau de acesso, ou seja, todos conhecem ou tem acesso a esta chave. Até mesmo o invasor a conhece? Sim! Pois, ela é utilizada apenas para criptografar mensagens

Chave privada: Privada no que se refere ao grau de acesso, ou seja, apenas o seu dono a conhece e não a divulga. Ela é utilizada para descriptografar as mensagens geradas pela sua chave pública correspondente.

As mensagens criptografadas com a chave pública só podem ser descriptografadas com a chave privada correspondente.

Exemplificando passo a passo uma troca de mensagens entre Wagner e Letícia.
Situação:

1. Wagner deseja enviar uma mensagem sigilosa, ou seja, secreta, para Letícia. Sabendo que a Internet não oferece um ambiente seguro, contrataram um serviço de segurança e ganharam duas chaves para trocar informações pela Internet.

2. Wagner pede a chave pública da Letícia, que pode ser enviada de qualquer maneira, pois mesmo que seja lida por outra pessoa, não teriam problemas (a chave pública permite apenas criptografar mensagens).

3. Após receber a chave púbica da Letícia, Wagner escreve, criptografa utilizando a chave pública da Letícia e envia a mensagem pela Internet;

4. Letícia recebe a mensagem criptografada e descriptografa a mensagem utilizando sua chave privada, que é apenas de seu conhecimento;

5. Agora, se Letícia quiser responder a mensagem, deverá realizar o mesmo procedimento, só que utilizando a chave pública do Wagner.

Certificado Digital

O certificado digital é um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade.

Exemplos semelhantes a um certificado digital são o CNPJ, RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição ou pessoa e a autoridade (para estes exemplos, órgãos públicos) que garante sua validade.

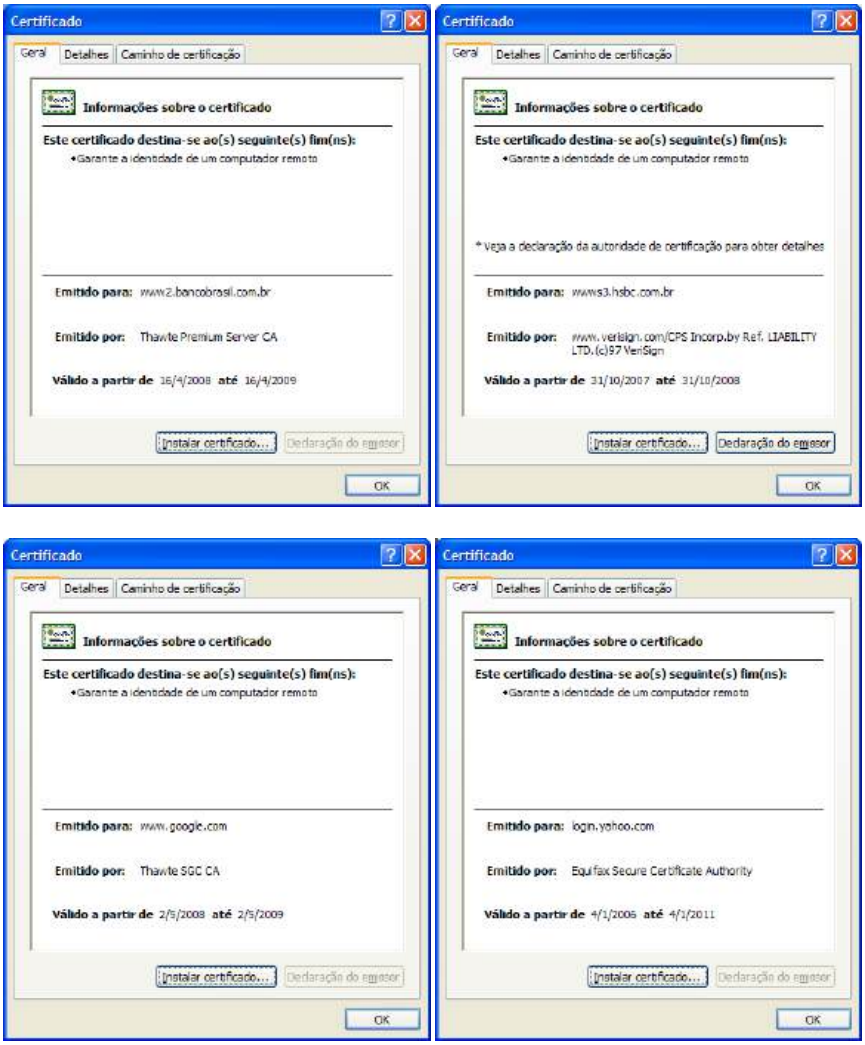
Algumas das principais informações encontradas em um certificado digital são:

- Para quem foi emitido (nome, número de identificação, estado, etc);
- Por quem foi emitido (Autoridade Certificadora (AC));
- O número de série e o período de validade do certificado;
- A assinatura digital da Autoridade Certificadora.

O objetivo da assinatura digital no certificado é indicar que outra entidade (a Autoridade Certificadora) garanta a veracidade das informações nele contidas. Destaca-se o princípio da Autenticidade e Integridade.

A partir de um certificado digital podemos afirmar que o site é legítimo e que seu conteúdo não foi alterado. Em outras palavras, o site está livre dos perigos oferecidos pelas técnicas *Pharming* e *Phishing*, que serão abordados mais adiante.

Veja alguns exemplos de certificados digitais:



Assinatura digital

A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se **o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada**. Destaca-se o princípio da Autenticidade e Integridade.

Desta forma, é utilizado o método de criptografia de chaves pública e privada, mas em um processo inverso.

Essa é simples, vamos inverter as chaves no processo usando o mesmo exemplo e perceba como é enviada uma mensagem assinada.
Situação:

1. Wagner deseja enviar uma mensagem assinada, ou seja, autêntica (garantir que a mensagem é enviada por ele e que não sofrerá alterações durante o envio), para Letícia. Sabendo que a Internet não oferece um ambiente seguro e muitos podem se passar por ele, Wagner contratou um serviço de segurança e ganhou duas chaves para trocar informações pela Internet.
2. Wagner escreve, criptografa utilizando a sua chave privada, onde será gerado um código (a assinatura digital), e envia a mensagem pela Internet;
3. Letícia recebe a mensagem criptografada e descriptografa a mensagem utilizando a chave pública do Wagner;

4. Neste momento será gerado um segundo código (assinatura digital), que será comparado com o primeiro;
5. Se os dois códigos (assinaturas digitais) forem idênticos, Letícia saberá que o remetente foi realmente o Wagner e que o conteúdo da mensagem não foi alterado.

É importante ressaltar que a segurança do método baseia-se no fato de que a chave privada é conhecida apenas pelo seu dono. Também é importante ressaltar que o fato de assinar uma mensagem não significa gerar uma mensagem sigilosa.

Para o exemplo anterior, se José quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

FIREWALLS (PAREDE DE FOGO)

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre seu computador e a Internet (ou entre a rede onde seu computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.

Explicando de maneira mais precisa, o firewall é um mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e a filtragem de dados. A vantagem do uso de firewalls em redes, é que somente um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

Há mais de uma forma de funcionamento de um firewall, que varia de acordo com o sistema, aplicação ou do desenvolvedor do programa. No entanto, existem dois tipos básicos de conceitos de firewalls: o que é baseado em filtragem de pacotes e o que é baseado em controle de aplicações. Ambos não devem ser comparados para se saber qual o melhor, uma vez que cada um trabalha para um determinado fim, fazendo que a comparação não seja aplicável.

- ***Filtragem de pacotes:*** O firewall que trabalha na filtragem de pacotes é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de firewall determina que endereços IPs e dados que podem estabelecer comunicação e/ ou transmitir/ receber dados. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados (como softwares de mensagens instantâneas, tal como o ICQ ou MSN Messenger). O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficazes o suficiente.

- ***Firewall de aplicação:*** Firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são conhecidos como Proxy

(Servidor Proxy consiste em um mecanismo de segurança que gerencia o tráfego de dados e pode oferecer também controle restrito de acesso).

O Windows XP já vem com um firewall, que apesar de não ser tão completo, é um bom aliado na segurança.

DoS - (Denial of Service- Negação de Serviço)

Os ataques de negação de serviço (DoS – *Denial of Service*) consistem em sobrecarregar **um sistema** com uma quantidade excessiva de solicitações. Sobrecarregando o sistema, o sistema para de atender novos pedidos de solicitações, efetivando a ação do Atacante.

Exemplos deste tipo de ataque são:

- Gerar uma grande sobrecarga no processamento de dados de um computador, de modo que o usuário não consiga utilizá-lo;
- Gerar um grande tráfego de dados para uma rede, ocupando toda a conexão disponível, de modo que qualquer computador desta rede fique indisponível;
- Tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários a suas caixas de correio no servidor de e-mail ou ao servidor Web.

DDoS (Distributed Denial of Service)

Constitui em um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação **um ou mais serviços ou computadores** conectados à Internet.

Normalmente estes ataques procuram ocupar toda a conexão disponível para o acesso a um computador ou rede, causando grande lentidão ou até mesmo indisponibilizando qualquer comunicação com este computador ou rede.

ATACANTES OU INVASORES

Hacker

É aquela pessoa com grande conhecimento computacional e na área da segurança computacional, que possui uma grande facilidade de análise, assimilação, compreensão e capacidades surpreendentes de conseguir fazer o que quiser (literalmente) com um computador. Ele sabe perfeitamente que nenhum sistema é completamente livre de falhas, e sabe onde procurar por elas, utilizando de técnicas das mais variadas (aliás, quanto mais variado, mais valioso é o conhecimento do Hacker). O termo: Hacker, originalmente, designava qualquer pessoa que fosse extremamente especializada em uma determinada área.

Cracker

Possui tanto conhecimento quanto os Hackers, mas com a diferença de que, para eles, não basta entrar em sistemas, quebrar senhas, e descobrir falhas. Eles precisam deixar um aviso de que estiveram lá, algumas vezes destruindo partes do sistema, e até aniquilando com tudo o que vêem pela frente. Também são atribuídos aos crackers programas que retiram travas em softwares, bem como os que alteram suas características, adicionando ou modificando opções, muitas vezes relacionadas à pirataria.

Lammer (Novato)

Lammer é aquele cara que quer aprender sobre Hackers. Não tem tanto conhecimento quanto os Hackers, mas utiliza os programas ou técnicas Hacker sem saber exatamente o que está fazendo.

Bancker

Possui tanto conhecimento quanto os Hackers, porém dedicam seu conhecimento para atividades fraudulento bancária, cartões de crédito e etc. Sempre visam obter informações financeiras dos usuários.

Phisher

Semelhante aos Bancker. Visam obter informações financeiras ou de acesso dos usuários. Utilizam diversas técnicas para obter essas informações. Desde o desenvolvimento de aplicativos maliciosos (Malware), que enviam as informações digitadas (Keyloggers) ou clicadas (Screenloggers) pelo usuário. Algumas técnicas dos Phishers incluem o carregamento de janelas pop up e direcionamento à sites falsos.

Spammer

Empresa ou indivíduo que envia e-mail para milhares de usuários (e-mails em massa). O conteúdo destas mensagens são publicidades, caracterizando o tipo de e-mail SPAM. Estas mensagens não solicitadas são enviadas para usuário onde tiveram seus e-mails vendidos ou obtidos por intermédio de ferramentas de busca específica de e-mails.

Defacer

Possui tanto conhecimento quanto os Hackers, utiliza seu conhecimento para invadir sites. Podem alterar as informações de um site ou apenas “pichar” o site com mensagens idealistas ou simplesmente vangloriando pelo feito.

Phreacker

É especializado em telefonia. Faz parte de suas principais atividades as ligações gratuitas (tanto local como interurbano e internacional), reprogramação de centrais telefônicas, instalação de escutas (não aquelas colocadas em postes telefônicos, mas imagine algo no sentido de, a cada vez que seu telefone tocar, o dele também o fará, e ele poderá ouvir sua conversa), etc. O conhecimento de um Phreaker é essencial para se buscar informações que seriam muito úteis nas mãos de mal-intencionados. Além de permitir que um possível ataque a um sistema tenha como ponto de partida, provedores de acessos em outros países, suas técnicas permitem não somente ficar invisível diante de um provável rastreamento.

CÓDIGOS MALICIOSOS

Aplicativos Maliciosos (Malware)

Aplicativo malicioso ou Malware (Malicious Software) é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador.

Na literatura de segurança o termo malware também é conhecido por "software malicioso".

Alguns exemplos de malware são:

- vírus;
- worms e bots;
- backdoors;
- cavalos de tróia;
- keyloggers e outros programas spyware;

Cavalos de Tróia

Cavalo de tróia (trojan horse) é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Tem como função abrir portas de acesso ao computador, desabitar ferramentas de segurança, enviar informações referentes ao computador do usuário como, por exemplo, endereço de IP, sistema operacional utilizado, navegador utilizado, portas que estão sendo utilizadas e etc. Estas informações são utilizadas pelo invasor para definir uma estratégia de invasão, pois, sabendo os pontos fracos (vulnerabilidades) desses programas poderá ser facilmente explorada pelo atacante.

Backdoors

Normalmente, um invasor procura garantir uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão e, é claro, sem ser notado.

A esses programas que facilitam o retorno de um invasor a um computador comprometido, utilizando serviços criados ou modificados para este fim, dá-se o nome de backdoor.

Adware e Spyware

Adware (Advertising software) é um tipo de software especificamente projetado para apresentar propagandas, seja através de um browser, seja através de algum outro programa instalado em um computador.

Em muitos casos, os adwares têm sido incorporados a softwares e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem software livre ou prestam serviços gratuitos. Um exemplo do uso legítimo de adwares pode ser observado no programa de troca instantânea de mensagens MSN Messenger.

Spyware, por sua vez, é o termo utilizado para se referir a uma grande categoria de software que tem o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros.

Existem adwares que também são considerados um tipo de spyware, pois são projetados para monitorar os hábitos do usuário durante a navegação na Internet, direcionando as propagandas que serão apresentadas.

Os spywares, assim como os adwares, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa.

Seguem algumas funcionalidades implementadas em spywares, que podem ter relação com o uso legítimo ou malicioso:

- Monitoramento de URLs acessadas enquanto o usuário navega na Internet;
- Alteração da página inicial apresentada no browser do usuário;
- Varredura dos arquivos armazenados no disco rígido do computador;
- Monitoramento e captura de informações inseridas em outros programas, como IRC ou processadores de texto;
- Instalação de outros programas spyware;
- Captura de senhas bancárias e números de cartões de crédito;
- Captura de outras senhas usadas em sites de comércio eletrônico.

É importante ter em mente que estes programas, na maioria das vezes, comprometem a privacidade do usuário e, pior, a segurança do computador do usuário, dependendo das ações realizadas pelo spyware no computador e de quais informações são monitoradas e enviadas para terceiros.

Keyloggers

Keylogger é um programa que duplica o que é digitado pelo usuário. Um arquivo é gerado e enviado para o e-mail do invasor ou para um servidor de arquivos. O atacante procura seqüência de informações como: Endereços de sites, nome de usuário, senhas, identidades de acesso, RG, CPF, endereços residenciais e comerciais, números de cartão de créditos (com código verificador e data de validade), etc...

Screenloggers

Screenlogger é um programa semelhante ao Keylogger, porém ao invés de colher informações digitadas pelo usuário, envia, em forma de imagem, a região clicada pelo usuário. Essa técnica visa obter informações que não seriam obtidas pelos Keyloggers, por exemplo, senhas clicadas em um teclado virtual e etc.

Worms

Worm é um programa independente com capacidade de se auto-propagar através de redes, enviando cópias de si mesmo de computador para computador, explorando a vulnerabilidade de programas e sistemas ou falhas na configuração de softwares instalados.

O Worm não é um vírus, pois não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar.

Pode abrir portas de acesso para entrada de novos Worms.

Vírus

Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção.

Os vírus criam cópias de si mesmo, espalhando-se pelo computador, dificultando a ação do antivírus.

Os vírus de computador podem gerar desde travamentos, lentidão, perda de dados e até mesmo danificar programas e arquivos.

Os principais tipos de vírus são:

- Vírus de arquivos: infectam arquivos de programas e criados pelo usuário;
- Vírus de boot: infectam os arquivos de inicialização do sistema, escondem-se no primeiro setor do disco e são carregados na memória antes do sistema operacional.
- Vírus de macro: comuns em arquivos do Word e Excel são vírus que ficam anexados ao arquivo.
- Vírus criptografados: são vírus que tem seu código fonte (linhas de comando) criptografadas, ou seja, os caracteres da programação são alterados por outros caracteres. Tudo isso para dificultar sua interpretação e conseqüentemente seu antídoto.
- Vírus polimórficos: destaca-se por multiplicarem-se com facilidade e para cada novo vírus gerado seu código fonte é alterado.

Spam

Spam é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciado como UCE (do inglês **U**nsolicited **C**ommercial **E**-mail – E-mail Comercial Não Solicitado).
Este e-mail contém propaganda, enganosa ou não. Podem conter vírus anexados à mensagem, bem como conter links que direcionam para arquivos maliciosos.

Boatos (Hoax)

Boatos (hoaxes) são e-mails que possuem conteúdos alarmantes ou falsos e que, geralmente, têm como remetente ou apontam como autora da mensagem alguma instituição, empresa importante ou órgão governamental. Através de uma leitura minuciosa deste tipo de e-mail, normalmente, é possível identificar em seu conteúdo mensagens absurdas e muitas vezes sem sentido.

Dentre os diversos boatos típicos, que chegam às caixas postais de usuários conectados à Internet, podem-se citar as correntes, pirâmides, mensagens sobre pessoas que estão prestes a morrer de câncer, entre outras.

Histórias deste tipo são criadas não só para espalhar desinformação pela Internet, mas também para outros fins maliciosos.

Phishing

Phishing, também conhecido como phishing scam, é um termo criado para descrever qualquer ação maliciosa que tenha como objetivo obter dados pessoais e financeiros do usuário.

As técnicas Phishing dão-se através do envio de mensagem não solicitada, se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso a páginas falsificadas, projetadas para furtar dados pessoais e financeiros de usuários.

A palavra phishing (de "fishing") vem de uma analogia criada pelos fraudadores, onde "iscas" (e-mails) são usadas para "pescar" senhas, dados pessoais e financeiros de usuários da Internet.

Atualmente, este termo vem sendo utilizado também para se referir aos seguintes casos:

- Mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetado para obter dados pessoais e financeiros (ex: Spyware, Keyloggers);
- Mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

Pharming

O Pharming é uma técnica que utiliza o seqüestro ou a "contaminação" do DNS (**D**omain **N**ame **S**ystem) para levar os usuários a um site falso, alterando o DNS do site de destino. O sistema também pode redirecionar os usuários para sites autênticos através de proxies controlados pelos Phishers, que podem ser usados para monitorar e interceptar a digitação.

Os sites falsificados coletam números de cartões de crédito, nomes de contas, senhas e números de documentos. Isso é feito através da exibição de um Pop-up para roubar a informação antes de levar o usuário ao site real. O programa mal-intencionado usa um certificado auto-assinado para fingir a autenticação e induzir o usuário a acreditar nele o bastante para inserir seus dados pessoais no site falsificado.

Outra forma de enganar o usuário é sobrepor a barra de endereço e status de navegador para induzi-lo a pensar que está no site legítimo e inserir suas informações.

Os phishers utilizam truques para instalar programas criminosos nos computadores dos consumidores e roubar diretamente as informações. Na maioria dos casos, o usuário não sabe que está infectado, percebendo apenas uma ligeira redução na velocidade do computador ou falhas de funcionamento atribuídas a vulnerabilidades normais de software. Um software de segurança é uma ferramenta necessária para evitar a instalação de programas criminosos se o usuário for atingido por um ataque.

Alguns veículos de divulgação descrevem Pharming como um tipo específico de Phishing.

Engenharia Social

Conhecido como a arte de enganar. É uma técnica utilizada pelo atacante para obter informações pessoais de um usuário. Existem casos onde o atacante se passa por outra pessoa ou empresa para obter estas informações.

QUESTÕES DE PROTEÇÃO E SEGURANÇA

(CESPE-UNB)

224. Atualmente, mensagens de correio eletrônico podem ser utilizadas para se enviar aplicativos maliciosos que, ao serem executados, acarretam aumento na vulnerabilidade de um computador e das possibilidades de ataque a um sistema. Entre esses aplicativos, encontram-se aqueles denominados vírus de computador, que podem ser definidos como sendo programas ou macros executáveis que, ao serem acionados, realizam atos não-solicitados e copiam a si mesmos em outros aplicativos ou documentos.

225. Na categoria de aplicativos maliciosos (*malware*), um *adware* é um tipo de software projetado para apresentar propagandas através de um browser ou de algum outro programa instalado no computador, podendo até mesmo carregar janelas *pop up* com algum tipo de propaganda.

226. O símbolo  , localizado na barra de status da janela do IE6, indica que a página web mostrada, ou a conexão que está sendo realizada, é do tipo segura, em que se garante o acesso ao site, livre do perigo oferecido pelas técnicas *pharming* ou *phishing*.

227. Para evitar que as informações obtidas em sua pesquisa, ao trafegarem na rede mundial de computadores, do servidor ao cliente, possam ser visualizadas por quem estiver monitorando as operações realizadas na Internet, o usuário tem à disposição diversas ferramentas cuja eficiência varia de implementação para implementação. Atualmente, as ferramentas que apresentam melhor desempenho para a funcionalidade mencionada são as denominadas *Keyloggers* e *Screenloggers* e os sistemas ditos *firewall*, sendo que, para garantir tal eficiência, todas essas ferramentas fazem uso de técnicas de *Sniffers* e *Backdoors* tanto no servidor quanto no cliente da aplicação Internet.

228. Um vírus de computador pode ser contraído no acesso a páginas web. Para se evitar a contaminação por vírus, é necessário que o navegador utilizado tenha um software antivírus instalado e ativado. Para se ativar o antivírus disponibilizado pelo IE6, é suficiente clicar o menu Ferramentas e, em seguida, clicar a opção Ativar antivírus.

229. Atualmente, mensagens de correio eletrônico podem ser utilizadas para se enviar aplicativos maliciosos que, ao serem executados, acarretam aumento na vulnerabilidade de um computador e das possibilidades de ataque a um sistema.

230. Existem diversos procedimentos ou mecanismos para impedir que aplicativos maliciosos anexados a uma mensagem de correio eletrônico sejam armazenados ou executados em um computador. Entre esses, pode-se destacar o uso do antivírus, que, ao ser instalado em um computador é capaz de decidir ativamente qual arquivo pode ou não ser executado, diminuindo as conseqüências de um ataque do tipo *phishing*.

231. Vírus de macro infectam a área do sistema de um disco, ou seja, o registro de inicialização em disquetes e discos rígidos.

232. Um vírus de computador pode ser contraído no acesso a páginas web. Para se evitar a contaminação por vírus, é necessário que o navegador utilizado tenha um *software* antivírus instalado e ativado. Para se ativar o antivírus disponibilizado pelo IE6, é suficiente clicar o menu Ferramentas e, em seguida, clicar a opção Ativar antivírus.

233. Considere a seguinte situação hipotética. Para que um cliente acesse os seus dados bancários por meio da Internet, o Banco do Brasil, para aumentar a segurança nesse acesso, passou a exigir o cadastramento do número MAC da *interface* de rede do computador utilizado pelo cliente no acesso ao sítio do banco. Nessa situação, é correto concluir que, para cada provedor de acesso que o cliente utilize para acessar o sítio do banco, novo cadastro deverá ser efetuado, pois, para cada provedor, haverá um número MAC específico.

234. O termo WORM é usado na informática para designar programas que combatem tipos específicos de vírus de computador que costumam se disseminar criando cópias de si mesmos em outros sistemas e são transmitidos por conexão de rede ou por anexos de e-mail.

235. A assinatura digital consiste na criação de um código de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

236. O *firewall* é o dispositivo que permite a conexão com a Internet, uma vez que é responsável pela conversão do sinal analógico em sinal digital.

237. *Trojan* é um programa que age utilizando o princípio do cavalo de tróia. Após ser instalado no computador, ele libera uma porta de comunicação para um possível invasor.

238. O termo TCP/IP denomina o grupo de aplicativos de computador que tem a função de detectar e eliminar a infecção de programas por vírus de computador.

239. *Adwares* são *softwares* maliciosos criados por programadores de vírus.

240. Caso um usuário envie uma mensagem de correio eletrônico e deseje que ela não possa ser lida por alguém que, por algum meio, a intercepte, ele deve se certificar que nenhum processo de criptografia seja usado para codificá-la.

241. Considerando que um teste de velocidade de conexão tenha sido realizado por meio de um computador que tenha ativado sistema antivírus e de um *firewall*, se estes sistemas fossem desativados, a velocidade de transmissão medida poderia atingir valores maiores que o obtido no teste mencionado.

(FCC)

242. Um *firewall* tradicional

a) Permite realizar filtragem de serviços e impor políticas de segurança.
b) Bem configurado em uma rede corporativa realiza a proteção contra vírus, tornando-se desnecessária a aquisição de ferramentas antivírus.
c) Protege a rede contra *bugs* e falhas nos equipamentos decorrentes da não atualização dos sistemas operacionais.
d) Evita colisões na rede interna e externa da empresa, melhorando, com isto, o desempenho do ambiente organizacional.
e) Deve ser configurado com base em regras permissivas (todos podem fazer tudo o que não for proibido), restringindo-se acessos apenas quando necessário, como melhor política de segurança.

243. Programa malicioso que, uma vez instalado em um microcomputador, permite a abertura de portas, possibilitando a obtenção de informações não autorizadas, é o:

a) *Firewall*.
b) *Trojan Horse*.
c) SPAM *Killer*.
d) Vírus de Macro.
e) Antivírus.

244. A respeito de assinatura e autenticação digital, analise as ocorrências abaixo:
I. Uso de uma de função *hash*;
II. Uso da chave privada;
III. Uso da chave pública;
IV. Envio dos dados de um usuário do sistema para outro usuário.
Na correta seqüência temporal, estritamente de um processo de assinatura digital tradicional (desconsiderando a criptografia da mensagem), temos:

a) O item I somente ocorrendo após o item II.
b) O item III somente ocorrendo após o item II.
c) O item I somente ocorrendo após o item IV.
d) O item I somente ocorrendo antes do item IV.
e) O item III somente ocorrendo antes do item IV.

245. Tradicionalmente realiza a proteção de máquinas de uma rede contra os ataques (tentativas de invasão) provindos de um ambiente externo. Trata-se de
a) Roteador. b) Antivírus. c) *Password*. d) *Firewall*. e) *Hub*.

246. No que diz respeito à proteção e à segurança em informática, analise as definições abaixo:
I. Procedimento para salvaguarda física de informações.
II. Palavra secreta que visa a restringir o acesso a determinadas informações.
III. Método de codificação de dados que visa a garantir o sigilo de informações.
Essas definições correspondem, respectivamente, a

a) *Layout*, criptograma e *restore*.
b) *Backup*, *password* e criptografia.
c) *Lookup*, *password* e *login*.
d) Criptografia, *login* e *backup*.
e) *Backup*, *plugin* e reprografia.

247. Os vírus que normalmente são transmitidos pelos arquivos dos aplicativos MS-Office são denominados tipo vírus de

a) Macro.
b) *Boot*.
c) E-mail.
d) Setor de inicialização.
e) Arquivo executável.

248. Uma senha se tornará frágil, ou será fácil de ser descoberta, caso na sua elaboração utilize

a) Um código, que seja trocado regularmente.
b) Pelo menos 8 caracteres entre letras, números e símbolos.
c) Nomes próprios ou palavras contidas em dicionários.
d) Um código fácil de ser lembrado.
e) Um código simples de digitar.

249. A pessoa que quebra ilegalmente a segurança dos sistemas de computador ou o esquema de registro de um *software* comercial é denominado:
a) *Hacker*. b) *Scanner*. c) *Finger*. d) *Cracker*. e) *Sniffer*.

250. Se a proteção contra vírus de macro do processador de texto estiver assinalada com nível de segurança "alto" e um documento que contenha "macros não assinadas" for aberto, o software antivírus do Oficce 2000 verificará o documento e

a) As macros serão desativadas automaticamente e o documento aberto.
b) As macros serão ativadas automaticamente e o documento aberto.
c) O usuário será solicitado a ativar ou desativar as macros.
d) O usuário será avisado de um possível vírus e as macros serão desativadas automaticamente.
e) Nenhum aviso será emitido e as macros serão ativadas.

251. A melhor forma de evitar que os sistemas operacionais e outros softwares instalados no computador possuam vulnerabilidades é

a) Instalar somente *softwares* originais e legais.
b) Instalar programas de proteção contra vírus e outros tipos de ataque.
c) Reinstalar os *softwares*, quando as vulnerabilidades forem detectadas.
d) Mantê-los protegidos contra o acesso de pessoas não autorizadas.
e) Mantê-los atualizados com a aplicação de *patches* específicos.

252. Selecione a melhor forma de privacidade para dados que estejam trafegando em uma rede:

a) Criptografia.
b) Chaves de segurança e bloqueio de teclados.
c) Emprego de sistema de senhas e autenticação de acesso.
d) Métodos de Backup e recuperação eficientes.
e) Desativação da rede e utilização dos dados apenas em "papel impresso".

253. Um conjunto de programas relacionados, alocados no servidor de uma rede de computadores, que protege os recursos privados dessa rede contra a intrusão ou acesso indesejável de usuários não autorizados é um
a) *Wallpaper*. b) *Homework*. c) *Scan* vírus. d) *Retro* vírus. e) *Firewall*.

254. Após instalar antivírus em uma rede,

a) Não é necessário proceder à "varredura" dos arquivos das estações se, porventura, estas adquirirem algum tipo de vírus.
b) Deve-se ativá-lo somente quando todas as estações de trabalho estiverem conectadas à rede.
c) Deve-se manter atualizada a lista de vírus.
d) Não é necessário instalar um *firewall* porque o antivírus já possui essa função embutida.
e) Deve-se instalar um *firewall*, caso contrário o antivírus não funcionará na rede.

255. Um _____ efetivamente coloca uma barreira entre a rede corporativa e o lado externo, protegendo o perímetro e repelindo *hackers*. Ele age como um único ponto de entrada, através do qual todo o tráfego que chega pela rede pode ser auditado, autorizado e autenticado. Completa corretamente a lacuna acima:

a) *Firewall*.
b) Antivírus.
c) Servidor Web.
d) Servidor de aplicativos.
e) *Browser*.

256. As ferramentas antivírus:

a) São recomendadas apenas para redes com mais de 100 estações.
b) Dependem de um *firewall* para funcionarem.
c) Podem ser utilizadas independente do uso de um *firewall*.
d) E um *firewall* significam a mesma coisa e têm as mesmas funções.
e) Devem ser instaladas somente nos servidores de rede e não nas estações de trabalho.

257. A criação de uma DMZ (*Delimitarized Zones*) é um recurso para melhorar a segurança associada ao mecanismo de proteção denominado.

a) Certificação digital.
b) Clusterização.
c) Antivirus.
d) *Firewall*.
e) Conformidade.

258. Assinale a opção que, no âmbito da segurança da informação, NÃO é um exemplo de vulnerabilidade.

a) Funcionário desonesto.
b) *Firewall* mal configurado.
c) Sistema operacional desatualizado.
d) *Links* sem contingência.
e) Rede elétrica instável.

259. Os procedimentos a seguir são recomendados para aumentar o nível de segurança do computador, EXCETO:

a) Não utilizar programas piratas.
b) Manter antivírus e *spyware* atualizados.
c) Instalar programas com procedência desconhecida.
d) Evitar o uso de dispositivos de armazenamento de terceiros.
e) Realizar periodicamente *backup* dos arquivos mais importantes.

260. Para executar tarefas comuns, que não exijam privilégios de administrador, é uma boa prática de segurança não utilizar um usuário que possua tais privilégios, uma vez que:

a) Cavalos de tróia só atacam máquinas autenticadas com administrador do sistema.
b) Um código malicioso pode ganhar os privilégios do usuário autenticado.
c) Programas antivírus só podem ser atualizados por usuários sem privilégios de administrador.
d) Usuários sem privilégio de administrador são imunes a código malicioso.
e) Usuários sem privilégios de administrador, apenas, possuem permissão para executar o navegador HTML.

261. NÃO é considerado um programa malicioso:

a) *Keylogger*
b) Trojan
c) *Worm*
d) Spyware
e) Firewall

262. Observe as seguintes afirmativas sobre segurança em senhas de acesso.
I. Todo vírus com extensão EXE instala um programa espião para roubo de senhas.
II. Quanto menor o tamanho de uma senha, maior sua segurança.
III. Quanto maior a aleatoriedade de uma senha, maior sua segurança.
Está(o) correta(s), somente, a(s) afirmativa(s):
a) I
b) II
c) III
d) I e III
e) II e III

263. Em programas de antivírus, heurísticas são utilizadas para:

a) Imunizar e-mails contaminados.
b) Bloquear conexões externas ao computador.
c) Atualizar automaticamente as estatísticas globais de infecção.
d) Detectar um vírus ainda desconhecido.
e) Restaurar o sistema operacional a um estado antes da infecção.

264. O arquivo que, anexado à mensagem de correio eletrônico, oferece, se aberto, O MENOR risco de contaminação do computador por vírus é:

a) copia.exe
b) happy.doc
c) love.com
d) vírus.jpg
e) renomeia.bat

265. Uma mensagem enviada de X para Y é criptografada e descriptografada, respectivamente, pelas chaves:

a) Pública de Y (que X conhece) e privada de X.
b) Pública de Y (que X conhece) e privada de Y.
c) Privada de X (que Y conhece) e privada de Y.
d) Privada de X (que Y conhece) e pública de X.
e) Privada de Y (que X conhece) e pública de X.

266. Sendo E (o Emissor) que envia uma mensagem sigilosa e criptografada, com a chave pública, para R (o Receptor), pode-se dizer que E codifica com a chave

a) Pública de R e R decodifica com a chave pública de E.
b) Pública de R e R decodifica com a chave privada de R.
c) Pública de E e R decodifica com a chave privada de R.
d) Privada de E e R decodifica com a chave pública de R.
e) Privada de E e R decodifica com a chave pública de E.

267. Observe a citação abaixo referente a um *malware* de computador:

"Programa intruso nos sistemas, normalmente de aparência inofensiva, mas que provoca uma ação maliciosa quando executado. Não tem capacidade de infectar outros arquivos ou se disseminar de um computador a outro. Para se introduzir em um sistema, deve ser deliberadamente enviado aos usuários, normalmente disfarçados como fotos, jogos e utilitários em geral. Possibilita que um intruso tome controle total do sistema invadido ou, até mesmo roube senhas e outras informações privadas."
O malware descrito é do tipo:
(A) *Hoax (Boatos)*
(B) *Trojan (Cavalo de Tróia)*
(C) *Worm (Verme)*
(D) *Keyloggers*
(E) *Sniffers (Farejador)*

(NCE)

268. Vírus de computador é:

a) Arquivo auto-executável que se instala no microcomputador, provocando desde travamento dos programas até a perda completa dos dados gravados nos discos.
b) Mau funcionamento do computador, causado pela umidade e mau contato entre as placas.
c) Instalação incorreta dos *softwares*.
d) Memória que carrega programa infectado.
Instalação incorreta de itens de *Hardware*.

Questões de Proteção e Segurança

			224. C	225. C	226. E	227. E	228. E	229. C	230. C
231. E	232. E	233. E	234. E	235. C	236. E	237. C	238. E	239. E	240. E
241. C	242. C	243. B	244. B	245. D	246. B	247. A	248. C	249. D	250. A
251. E	252. A	253. E	254. C	255. A	256. C	257. D	258. A	259. C	260. C
261. E	262. C	263. D	264. D	265. B	266. B	267. B	268. A		

Questões adicionais

Segurança da Informação

1. Tipos de Ataques

1) Analista Administrativo – Tecnologia da Informação - Administração de Rede e Segurança de Informações- Agência Nacional de Águas (03-2009) O(A) _____ representa um ataque que compromete diretamente a disponibilidade. Assinale a opção que completa corretamente a frase acima.

a) cavalo de tróia b) falsificação c) negação de serviço.
d) phishing e) sniffing

2) Analista de Finanças e Controle - Tecnologia da Informação – CGU (2004) Existe uma forma muito poderosa de ataque a um sistema denominada **DDoS**, cujo principal objetivo é:

a) inserir usuários não autorizados em um sistema.
b) executar aplicativos em um sistema com os privilégios de outro usuário.
c) enganar um servidor de um serviço de rede ao informá-lo um endereço falso durante o processo de autenticação ou solicitação de informações.
d) provocar uma sobrecarga com um número inesperado de acessos a um site, o que torna o carregamento de suas páginas mais demorado e sujeito a erros, provocando, em alguns casos, a interrupção dos seus serviços.
e) permitir acesso ao sistema pelo seu próprio projetista, utilizando uma porta introduzida por ele durante o processo de desenvolvimento, com a finalidade de furar a segurança normal implementada pela política de segurança.

3) Analista de Finanças e Controle - Tecnologia da Informação – CGU (2004) Analise as seguintes afirmações relativas à segurança na Internet:

I. **Engenharia Social** é um termo utilizado para descrever um método de ataque onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

II. **Vulnerabilidade** pode ser definida como uma falha no projeto ou implementação de um software que, quando explorada por um atacante,resulta na violação da segurança de um sistema.

III. Um **vírus de macro** normalmente é recebido como um arquivo executável anexado a uma mensagem de correio eletrônico. O conteúdo dessa mensagem procura induzir o usuário a clicar sobre o arquivo anexado, fazendo com que o vírus seja executado.

IV. Engenharia reversa é uma das principais técnicas adotadas por hackers para ter acesso não autorizado a computadores ou informações.

Estão corretos os itens:

a) I e II b) II e III c) III e IV
d) I e III e) II e IV

2. Malwares (Softwares Maliciosos)

4) Analista Administrativo – Tecnologia da Informação - Administração de Rede e Segurança de Informações- Agência Nacional de Águas (03-2009) O código malicioso caracterizado por ser executado independentemente, consumindo recursos do hospedeiro para a sua própria manutenção, podendo propagar versões completas de si mesmo para outros hospedeiros, é denominado:

a) vírus. b) backdoor. c) cookie.
d) verme. e) spyware.

5) TRF (2006) Analise as seguintes afirmações relacionadas a vírus e antivírus.

I. Um **cookie** é um vírus do tipo malware que pode ser armazenado pelo browser se um website requisitar. A informação não tem um tamanho muito grande e, quando acionados, alteram a configuração de segurança do browser.

II. Qualquer malware que possua um **backdoor** permite que o computador infectado seja controlado totalmente ou parcialmente através de um canal de IRC ou via conexão com uma porta.

III. O **Cavalo de Tróia** é um programa que, explorando deficiências de segurança de computadores, propaga-se de forma autônoma, contaminando diversos computadores geralmente conectados em rede. O Cavalo de Tróia mais conhecido atacou quantidades imensas de computadores na Internet durante os anos 90.

IV. A **Engenharia Reversa** é a arte de reverter códigos já compilados para uma forma que seja legível pelo ser humano. Técnicas de engenharia reversa são aplicadas na análise de vírus e também em atividades ilegais, como a quebra de proteção anticópia. A engenharia reversa é ilegal em diversos países, a não ser que seja por uma justa causa como a análise de um malware.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II b) II e III c) III e IV
d) I e III e) II e IV.

6) Auditor Fiscal da Receita Federal - Tecnologia da Informação - Prova 3 - Gabarito 1 (2005) Em relação a vírus de computador é correto afirmar que, entre as categorias de malware, o **Cavalo de Tróia** é um programa que:

a) usa um código desenvolvido com a expressa intenção de se replicar. Um Cavalo de Tróia tenta se alastrar de computador para computador incorporando-se a um programa hospedeiro. Ele pode danificar o hardware, o software ou os dados. Quando o hospedeiro é executado, o código do Cavalo de Tróia também é

executado, infectando outros hospedeiros e, às vezes, entregando uma carga adicional.

b) parece útil ou inofensivo, mas que contém códigos ocultos desenvolvidos para explorar ou danificar o sistema no qual é executado. Os cavalos de tróia geralmente chegam aos usuários através de mensagens de e-mail que disfarçam a finalidade e a função do programa. Um Cavalo de Tróia faz isso entregando uma carga ou executando uma tarefa mal-intencionada quando é executado.

c) usa um código mal-intencionado auto-propagável que pode se distribuir automaticamente de um computador para outro através das conexões de rede. Um Cavalo de Tróia pode desempenhar ações nocivas, como consumir recursos da rede ou do sistema local, possivelmente causando um ataque de negação de serviço.

d) pode ser executado e pode se alastrar sem a intervenção do usuário, enquanto alguns variantes desta categoria de malware exigem que os usuários executem diretamente o código do Cavalo de Tróia para que eles se alastrem. Os Cavalos de Tróia também podem entregar uma carga além de se replicarem.

e) não pode ser considerado um vírus ou um verme de computador porque tem a característica especial de se propagar. Entretanto, um Cavalo de Tróia pode ser usado para copiar um vírus ou um verme em um sistema-alvo como parte da carga do ataque, um processo conhecido como descarga. A intenção típica de um Cavalo de Tróia é interromper o trabalho do usuário ou as operações normais do sistema. Por exemplo, o Cavalo de Tróia pode fornecer uma porta dos fundos no sistema para que um hacker roube dados ou altere as definições da configuração.

7) Analista de Finanças e Controle - Prova P.3 - Tecnologia da Informação – CGU (2006) É crescente o número de incidentes de segurança causados por **vírus de computador e suas variações**. Com isso, as organizações estão enfrentando o problema com o rigor e cuidados merecidos. Nesse contexto, é correto afirmar que:

a) cavalos de tróia são variações de vírus que se propagam e possuem um mecanismo de ativação (evento ou data) e uma missão.

b) vírus polimórficos suprimem as mensagens de erro que normalmente aparecem nas tentativas de execução da atividade não-autorizada, utilizando, muitas vezes, criptografia para não serem detectados por anti-vírus.

c) os vírus de macro utilizam arquivos executáveis como hospedeiros, inserindo macros com as mesmas funções de um vírus em tais arquivos.

d) vírus geram cópias de si mesmo a fim de sobrecarregarem um sistema, podendo consumir toda a capacidade do processador, memória ou espaço em disco, eventualmente.

8) Auditor Fiscal da Receita Federal - Tecnologia da Informação - Prova 3 - Gabarito 1 (2005) Com relação à segurança e a ataques em redes de computadores, pode-se observar que, depois que um malware alcança uma máquina hospedeira, geralmente executará uma ação conhecida como carga. O tipo de carga conhecido como "**Porta dos fundos**"

a) é um tipo de carga de malware particularmente preocupante porque é normalmente desenvolvida para roubar informações. Se uma carga puder comprometer a segurança de um computador hospedeiro, é possível que ele desenvolva um mecanismo para passar informações para os responsáveis pelo malware.

b) é um dos tipos de carga mais destrutivos, normalmente um código mal-intencionado que altera ou exclui dados, tornando as informações no computador do usuário inúteis.

c) é um do tipo DoS, isto é, uma investida computadorizada feita por um invasor para sobrecarregar ou parar os serviços de uma rede, como um servidor da WEB ou um servidor de arquivos.

d) é um ataque DDoS que visa a simplesmente tornar um serviço específico temporariamente indisponível.

3. Agentes de Segurança

9) Um **Firewall** pode ser definido como uma coleção de componentes, colocada entre duas redes, que coletivamente possua propriedades que:

a) independentemente da política de segurança adotada, tem como objetivo principal impedir a entrada de vírus em um computador, via arquivos anexados a e-mails.

b) garantem que todo o tráfego de dentro para fora da rede, e vice-versa, deve ser bloqueado, independentemente da política de segurança adotada. Todo firewall deve ser à prova de violação.

c) garantem que todo o tráfego de dentro para fora da rede, e vice-versa, passe por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o firewall e, finalmente, ele deve ser à prova de violação.

d) garantem que apenas o tráfego de dentro para fora da rede deve passar por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o firewall e, fi nalmente, ele deve ser à prova de violação.

e) garantem que apenas o tráfego de fora para dentro da rede deve passar por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o firewall e, fi nalmente, ele deve ser à prova de violação.

4. Princípios da Segurança da Informação

10) Analista de Planejamento e Orçamento – MPOG (06-2008) A segurança da informação tem como objetivo a preservação da:

a) confi dencialidade, interatividade e acessibilidade das informações.

b) complexidade, integridade e disponibilidade das informações.

c) confidencialidade, integridade e acessibilidade das informações.

d) universalidade, interatividade e disponibilidade das informações.

e) confidencialidade, integridade e disponibilidade das informações.

11) Auditor Fiscal da Previdência Social – Prova 1 – INSS (2002) Uma informação, para ser considerada segura, precisa manter seus aspectos de confidenciabilidade, integridade e disponibilidade. A confidenciabilidade é a

a) propriedade de evitar a negativa de autoria de transações por parte do usuário, garantindo ao destinatário o dado sobre a autoria da informação recebida.
b) garantia de que o sistema se comporta como esperado, em geral após atualizações e retificações de erro.
c) análise e responsabilização de erros de usuários autorizados do sistema.
d) garantia de que as informações não poderão ser acessadas por pessoas não autorizadas.
e) propriedade que garante o acesso às informações através dos sistemas oferecidos.

12) Auditor Fiscal da Receita Estadual – Provas 1 e 2 – SEFAZ-CE (2006) Nos sistemas de Segurança da Informação, existe um método que _____. Este método visa garantir a integridade da informação. Escolha a opção que preenche corretamente a lacuna acima.

a) valida a autoria da mensagem
b) verifica se uma mensagem em trânsito foi alterada
c) verifica se uma mensagem em trânsito foi lida por pessoas não autorizadas
d) cria um backup diferencial da mensagem a ser transmitida
e) passa um antivírus na mensagem a ser transmitida

13) Auditor Fiscal da Receita Estadual – Provas 1 e 2 – SEFAZ-CE (2006) Analise as seguintes afirmações relacionadas a conceitos básicos de Segurança da Informação.

I. Um **firewall**, instalado entre uma rede LAN e a Internet, também é utilizado para evitar ataques a qualquer máquina desta rede LAN partindo de máquinas da própria rede LAN.

II. A **confidenciabilidade** é a propriedade de evitar a negativa de autoria de transações por parte do usuário, garantindo ao destinatário o dado sobre a autoria da informação recebida.

III. Na **criptografia** de chaves públicas, também chamada de criptografia assimétrica, uma chave é utilizada para criptografar e uma chave diferente é utilizada para decriptografar um arquivo.

IV. Uma das finalidades da **assinatura digital** é evitar que alterações feitas em um documento passem sem ser percebidas. Nesse tipo de procedimento, o documento original não precisa estar criptografado.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II b) II e III c) III e IV
d) I e III e) II e IV

14) Técnico Administrativo – MPU gabarito 1 (2004) Analise as seguintes afirmações relativas à segurança da informação.

I. A **disponibilidade** assegura que a informação será acessível somente por quem tem autorização de acesso.

II. Para garantir a **segurança da informação**, é necessário que os princípios básicos de confidencialidade, integridade e risco sejam respeitados.

III. A **integridade** assegura que a informação não foi alterada durante o processo de transporte.

IV. **Vírus de macro** infectam a área do sistema de um disco, ou seja, o registro de inicialização em disquetes e discos rígidos.

Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II b) II e III c) III e IV
d) II e IV e) I e III

15) Auditor Fiscal da Receita Federal - Tecnologia da Informação - Prova 3 - Gabarito 1 (2005) Alguns tipos de malware tentam atingir um objeto portador, também conhecido como hospedeiro, para infectá-lo. O número e tipo de objetos portadores que são alvos variam com as características dos malwares. Entre os portadores-alvo mais comuns, **as macros**:

a) são arquivos localizados em áreas específicas dos discos do computador (discos rígidos e mídias removíveis inicializáveis), como o registro mestre de inicialização (MBR).
b) são arquivos que suportam linguagens como Microsoft Visual Basic® Script, JavaScript, AppleScript ou PerlScript. As extensões dos arquivos desse tipo são: .vbs, .js, .wsh e .prl.
c) são o alvo do vírus "clássico" que é replicado anexando-se a um programa hospedeiro. Além dos arquivos típicos que usam a extensão das macros, arquivos com as seguintes extensões também podem ser usados com essa finalidade: .com, .sys, .dll, .ovl, .ocx e .prg.
d) são arquivos que suportam uma linguagem script de macro de um aplicativo específico, como um processador de texto, uma planilha eletrônica ou um aplicativo de banco de dados. Por exemplo, os vírus podem usar as linguagens de macro no Microsoft Word para causar vários efeitos, que podem variar de prejudiciais, como trocar palavras ou mudar as cores em um documento, a mal-intencionados, como formatar o disco rígido do computador.
e) são arquivos localizados no registro de inicialização do DOS e são capazes de executar códigos mal-intencionados. Quando o registro de um disco de inicialização é infectado, a replicação será efetivada se ele for usado para iniciar os sistemas de outros computadores.

16) Analista de Finanças e Controle - Tecnologia da Informação – CGU (2004) Analise as seguintes afirmações relativas aos conceitos de Segurança da Informação:

I. **Cofidencialidade** é a propriedade de manutenção do sigilo das informações. É uma garantia de que as informações não poderão ser acessadas por pessoas não autorizadas.

II. **Irretratabilidade** é a propriedade de evitar a negativa de autoria de transações por parte de usuários, garantindo ao

destinatário o dado sobre a autoria da informação recebida.

III. **Autenticidade** é a proteção da informação contra acessos não autorizados.

IV. **Isolamento ou modularidade** é a garantia de que o sistema se comporta como esperado, em especial após atualizações ou correções de erro.

Estão corretos os itens:
a) I e II b) II e III c) III e IV
d) I e III e) II e IV

17) Analista de Finanças e Controle - Tecnologia da Informação – CGU (2004) Considere um sistema no qual existe um conjunto de informações disponível para um determinado grupo de usuários denominados "auditores". Após várias consultas com respostas corretas, em um determinado momento, um usuário pertencente ao grupo "auditores" acessa o sistema em busca de uma informação e recebe, como resposta à sua consulta, uma informação completamente diferente da desejada. Neste caso houve uma falha na segurança da informação para este sistema na propriedade relacionada à:
a) Confidencialidade b) Integridade c) Auditoria
d) Disponibilidade e) Privacidade

18) Analista de Finanças e Controle - Tecnologia da Informação – CGU (2004) Considere um sistema no qual existe um conjunto de informações disponível para um determinado grupo de usuários denominados "auditores". Após várias consultas com respostas corretas e imediatas, em um determinado momento, um usuário pertencente ao grupo "auditores" acessa o sistema em busca de uma informação já acessada anteriormente e não consegue mais acessá-la. Neste caso houve uma falha na segurança da informação para este sistema na propriedade relacionada à
a) Privacidade b) Integridade c) Consistência
d) Irretratabilidade e) Disponibilidade

5. Criptografia, Assinatura Digital, Hash

19) Ciências da Computação - Tribunal de Contas-PI (03-2005) Sendo E (o Emissor) que envia uma mensagem sigilosa e criptografada, com chaves pública e privada, para R (o Receptor), pode-se dizer que E codifica com a chave
a) pública de R e R decodifica com a chave pública de E.
b) pública de R e R decodifica com a chave privada de R.
c) pública de E e R decodifica com a chave privada de R.
d) privada de E e R decodifica com a chave pública de R.
e) privada de E e R decodifica com a chave pública de E.

20) Analista - Área: Orçamento - MPU – Gabarito 4 (2004) Analise as seguintes afirmações relativas a conceitos de proteção e segurança da informação.

I. Um **ataque** é qualquer tentativa de penetrar em um sistema sem autorização. Os ataques podem ser classificados como ativos, quando alteram o conteúdo de uma mensagem, ou passivos, quando somente copiam seu conteúdo.

II. A **autenticação** é o processo destinado a verificar a validade de determinada mensagem.

III. A **assinatura digital** é uma técnica para converter um texto claro em texto criptografado.

IV. A **criptografia** gera um valor associado a uma determinada mensagem, que a garante contra falsificação. Um exemplo de criptografia são os dígitos de controle usados em conjunto com os números de conta corrente dos bancos.

Indique a opção que contenha todas as afirmações verdadeiras.
a) I e III b) II e III c) III e IV
d) I e II e) II e IV

21) Prova 1 – Comum – ENAP MPOG (05-2006) Uma **assinatura digital** é um meio pelo qual
a) o gerador de uma mensagem, de um arquivo ou de outras informações codificadas digitalmente vincula sua identidade às informações.
b) os servidores de e-mail substituem uma mensagem pelo equivalente codificado.
c) os servidores de páginas da Web identificam o endereço IP do site de destino.
d) os servidores de páginas da Web identificam o endereço IP do site de origem.
e) os Firewalls utilizam para garantir o repúdio da informação.

22) Prova 1 – Comum – ENAP MPOG (05-2006) Quanto aos conceitos básicos de Segurança da Informação é correto afirmar que a criptografia simétrica:
a) usa um algoritmo de criptografia que requer que a mesma chave secreta seja usada na criptografia e na decriptografia.
b) é um método de criptografia no qual duas chaves diferentes são usadas: uma chave pública para criptografar dados e uma chave particular para decriptografá-los.
c) é um método de criptografia no qual duas chaves diferentes são usadas: uma chave particular para criptografar dados e uma chave pública para decriptografá-los.
d) é o processo de regravação de partes de um arquivo em setores contíguos de um disco rígido a fim de aumentar a segurança da informação.
e) é o resultado de tamanho fixo, também chamado de síntese da mensagem, obtido pela aplicação de uma função matemática unidirecional a uma quantidade de dados arbitrária.

6. Extra

23) Assessor Especializado – IPEA (11-2004) O método de criptografia por chave assimétrica, entre dois pontos em comunicação, baseia-se somente na utilização de

a) uma chave secreta única para as duas pontas.
b) uma chave pública única para as duas pontas.
c) duas chaves secretas, uma para cada ponta.
d) duas chaves públicas, uma para cada ponta.
e) uma chave secreta individual e uma chave pública comum para cada uma das pontas.

24) Análise de Sistemas - TRT 24ª região (03-2006) Segundo a NBR ISO/IEC 17799:2001, o conceito de segurança da informação é caracterizado pela preservação de:
(I) que é a garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
(II) que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
(III) que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Preenchem correta e respectivamente as lacunas I, II e III:
a) disponibilidade − integridade – confidencialidade.
b) confidencialidade − integridade – disponibilidade.
c) integridade − confidencialidade − disponibilidade
d) confidencialidade − disponibilidade − integridade
e) disponibilidade − confidencialidade − integridade

25) Ciências da Computação - Tribunal de Contas-PI (03-2005) Os antivírus são programas que NÃO têm capacidade de
a) identificar e eliminar a maior quantidade de vírus possível.
b) analisar os arquivos obtidos pela Internet.
c) evitar o acesso não autorizado a um backdoor instalado.
d) verificar continuamente os discos rígidos e disquetes.
e) procurar vírus em arquivos anexados aos e-mails.

26) Técnico Legislativo – Agente de Polícia – Câmara dos Deputados (07-2007) Um programa capaz de se auto-propagar automaticamente através de redes, enviando cópias de si mesmo, de computador para computador, denomina-se
a) cavalo de tróia. b) macro. c) backup.
d) backdoor. e) worm.

27) Analista de Controle Externo – TI - TCE-AM (05-2008) Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador é o
a) Worm. b) Spyware. c) Backdoor.
d) Keylogger. e) Cavalo de Tróia.

28) Técnico Judiciário – TRT 8ª região (12-2004) As ferramentas antivírus:
a) são recomendadas apenas para redes com mais de 100 estações.
b) dependem de um firewall para funcionarem.
c) podem ser utilizadas independentes do uso de um firewall.
d) e um firewall significam a mesma coisa e têm as mesmas funções.
e) devem ser instaladas somente nos servidores de rede e não nas estações de trabalho.

29) Análise de Sistemas – TJ-PE (05-2007) Uma pessoa mal intencionada tenta obter informações como números de cartões de crédito, senhas, dados de contas ou outras informações pessoais convencendo-o a fornecê-las sob pretextos enganosos em um ataque via WEB do tipo
a) phishing scam. b) adware.
c) slice and dice. d) spyware. e) hijack.

1.C	2.D	3.A	4.D	5.E	6.B	7.D	8.A	9.C	10.E
11.D	12.B	13.C	14.B	15.D	16.A	17.B	18.E	19.B	20.D
21.A	22.A	23.E	24.B	25.C	26.E	27.D	28.C	29.A	